Republic of Panama
Superintendency of Banks

OTHER REPORTING ENTITIES AML RULE N°. 1-2019
(dated 26 March 2019)

"Whereby the Red Flags Catalog for Detecting Suspicious Operations related to Money Laundering, the Financing of Terrorism and the Financing of the Proliferation of Weapons of Mass Destruction for Money Service Businesses and Exchange Bureaus is established"

THE BOARD OF DIRECTORS
in use of its legal powers and,

WHEREAS:

Due to the issuance of Decree Law 2 dated 22 February 2008, the Executive Branch re-edited Decree Law 9 dated 26 February 1998 and all its amendments as a consolidated text, and this text was approved by means of Executive Decree 52 dated 30 April 2008, hereinafter referred to as the Banking Law;

Paragraph 2 of Article 5 of the Banking Law establishes that strengthening and fostering favorable conditions for the development of the Republic of Panama as an international financial center is an objective of the Superintendency of Banks;

Pursuant to Article 4 of the Banking Law, the Superintendency of Banks will have exclusive competence to regulate and supervise the banks, the banking business and other entities and activities assigned to it by other laws;

Law 23 dated 27 April 2015 adopted measures for the prevention of money laundering, the financing of terrorism and financing the proliferation of weapons of mass destruction;

Article 19 of Law 23 dated 27 April 2015 establishes the Superintendency of Banks, among others, as a supervisory body;

Paragraph 7 of Article 20 of Law 23 of 2015 provides that issuing guidance and feedback standards to the financial reporting entities, the nonfinancial reporting entities and activities performed by professionals subject to supervision for its enforcement, as well as the procedures for the identification of the final beneficiaries of legal entities and other legal arrangements, is among the duties of the supervisory bodies;

Pursuant to the provisions of Article 22 of Law 23 of 2015, the Superintendency of Banks is responsible for supervising financial reporting entities, among which are money service businesses, whether or not it is their principal activity, and exchange bureaus in any of their forms, whether operating by physical transfer or the purchase of future contracts, and whether or not it is their main activity, in matters of the prevention of money laundering, the financing of terrorism and the financing of the proliferation of weapons of mass destruction the financial reporting entities;

By means of Other Reporting Entities AML Rule 4-2018, dated 23 October 2018, the guidelines for preventing the misuse of services provided by money service businesses related to the prevention of money laundering, the financing of terrorism and the financing of the proliferation of weapons of mass destruction were established;

By means of Other Reporting Entities AML Rule 5-2018, dated 11 December 2018, the guidelines for preventing the misuse of services provided by exchange bureaus related to the prevention of money laundering, the financing of terrorism and the financing of the proliferation of weapons of mass destruction were established;

By means of Administrative Resolution 33-2018 dated 25 September 2018, the Financial Analysis Unit (UAF, for its acronym in Spanish) adopted and disseminated to Supervisory Bodies the Guidelines and Compendia of relevant risk indicators for the money service businesses and

exchange bureaus for detecting the financing of terrorism as a useful tool for strengthening the fight against the financing of terrorism, making due diligence measures more robust and providing guidance on the techniques and mechanisms used in the financing of terrorism;

During its working sessions, the Board of Directors determined it was necessary and advisable to establish, by means of a Rule, a Red Flags Catalog to prevent money laundering, the financing of terrorism and the financing of the proliferation of weapons of mass destruction, adjusted to the nature of the money service businesses and exchange bureaus' business to support and provide guidance to these financial reporting entities.

RESOLVES:

CHAPTER I
GENERAL OUTLINES

ARTICLE 1. SCOPE. The provisions herein will be applicable to the following reporting entities:

a. Money service businesses, whether or not it is the main activity;
b. Exchange bureaus, in any of their forms, whether operating by physical transfer or the purchase of future contracts, and whether or not it is their main activity.

ARTICLE 2. RED FLAGS CATALOG. The red flags catalog below must be adopted, for the purpose of money service businesses and exchange bureaus detecting and/or preventing suspicious operations related to money laundering, the financing of terrorism and the financing of the proliferation of weapons of mass destruction.

The red flags catalog contained herein provides examples of operations susceptible to being connected to money laundering, the financing of terrorism and the financing of the proliferation of weapons of mass destruction, without prejudice of other models that the reporting entity may establish.

ARTICLE 3. RED FLAGS ANALYSIS. The money service businesses and exchange bureaus must define specific criteria related to the red flags, depending on the nature of their operations. These reporting entities must also analyze, with special attention, any and all operations or behavior contained herein in order to determine, taking into consideration other signs, factors and criteria, whether they are suspicious operations related to the risks of money laundering, the financing of terrorism and the financing of the proliferation of weapons of mass destruction.

CHAPTER II
RED FLAGS IN GENERAL

ARTICLE 4. RED FLAGS RELATED TO CUSTOMER IDENTIFICATION. Reporting entities must pay special attention to the following behaviors or actions by customers:

1. **Formal identification:**

1.1. **Document:**

a. The customer that wants to use a document that raises the entity´s doubts on its consistency and/or veracity, that may have been altered, including a photograph or a customer's description that does not match his appearance, is expired, is a copy instead of the original, or whose issuance date does not match the document condition related to its wear and tear.

b. A customer that is just about to finish an operation and decides not to complete it or changes the amount of the operation when finding out that he is required to show an identification document;

c. The customer refuses to or is unable to provide the identification document or the personal data required by the establishment;

d. Every time the customer conducts an operation he provides different data on his identity, e.g.:

i. Gives different names or spells the name differently or changes his surnames order or how they are spelled out;

ii. Gives a different address or contact data or spells it differently or changes the numbers;

iii. Gives another identification document.

1.2. **Customer's nationality or residence:**

a. A customer or registered agent or a citizen in/from countries or territories classified as high-risk countries (especially those known as centers for money laundering, as producers of narcotic substances or for harboring terrorist groups) or countries with financial secrecy.

1.3. **Front men:**

a. A customer that says or pretends that he is not acting on his own behalf, or acts as the presenter of another person in an attempt to evade the entity's due diligence measures;

b. A customer who appears to be directed by a third party, particularly when he seems unaware of the full details of the operation being conducted;

c. Use of third parties to conduct operations for the sole purpose of receiving funds from abroad and transferring them to other recipients abroad;

d. An occasional customer that exchanges cash in one currency for another for tourism or travels, but appears to act following instructions from a third party.

1.4. **Wire transfer beneficiary:**

a. A customer who is nervous, has doubts or has to ask for information before furnishing the information required on the wire transfer beneficiary;

b. A customer that is clearly using phony remittance names (e.g. famous actors or singers);

c. Remittances in which it impossible or very hard to get the data on the beneficiary;

d. A report from the payer or receiver of the transaction at the destination warning the sender that a beneficiary is receiving remittances from other fund remitters, or is indicated on a list of criminals or is wanted by law enforcement agencies in his country [of origin].

1.5. **Others:**

a. A customer with published police or criminal records (e.g. published/posted in the media) or that is involved with or related to people subject to a ban on running operations or is linked to terrorism financing activities;

b. A customer that may be considered to be a politically exposed person or who is known to be a family member or associate of [a PEP], who tries to avoid the submittal of documents required to conduct the requested operation.

2. **Physical identification (knowing the customer's activity):**

   a. There are doubts as to the truthfulness of the data provided by the customer on his activity or the origin or destination of funds;

   b. Operations that because of their amount or frequency, do not belong to the customer's economic status or the proceeds from the activity he is engaged into;

   c. A businessman acting as customer:

      i. Participates in operations that are usually conducted with high denomination bills when the characteristics of the activity do not justify that use;

      ii. Orders wire transfers to people in other countries without having an apparent business reason or gives an incoherent explanation on the nature of the business or activity;

      iii. Receives wire transfers from people in other countries without having an apparent business reason or gives an incoherent explanation on the nature of the business or activity;

      iv. Refuses to provide full information on the type of business, purpose of the operation or any other information required by the reporting entity.

   d. Customers using generalities such as savings, work, sale, etc. to define the origin of their funds, without any reference to the operation or activity producing the funds;

   e. A customer that is about to conduct an operation and, when finding out that he is required to provide additional information, decides not to do it or changes its amount to try to avoid this requirement.

ARTICLE 5. RED FLAGS RELATED TO OPERATIONAL CHARACTERISTICS OR CUSTOMER BEHAVIOR. The reporting entities must pay special attention to the following behavior or actions involving structuring or fractioning of operations (individually or jointly) and the avoidance of thresholds requiring a specific follow-up on the customers conducting the following operations:

1. A customer or customers who, alone or in a concerted manner, carry out repeated operations over time for amounts under five thousand balboas (B/.5,000.00) or close to that amount in order to prevent the reporting entities detecting remittance or currency exchange patterns, complying with the requirements to provide additional information or systematic reporting, especially when it involves wire transfers having the same beneficiary from different ordering parties or that are addressed to high-risk areas or countries known for their relationship with money laundering, the financing of terrorism and/or the financing of the proliferation of weapons of mass destruction;

2. Customers sending wire transfers to different people within the same family when the customer is not a member of that family;

3. Customers going in a group, each party ordering operations of similar characteristics, especially if they receive instructions from one of them or from a third party;

4. Wire transfers received and sent by the same customer on the same date or close dates;

5. A customer that is the beneficiary of multiple wire transfers that seem to be remitted in a way designed to avoid having to provide additional information or requiring reporting:

   a. The same ordering party, each transfer just below the threshold required to trigger a specific follow up;

b. Orders from multiple parties from the same establishment, placing orders within a couple of minutes of each other and all just below the threshold required to trigger a specific follow up.

6. Customers that decide not to fulfill an operation or change the amount to avoid the threshold that requires them to provide additional information;

7. Customers ordering operations with the same characteristics (amount, country of destination, city of destination, etc.) of those ordered by other customers shortly before them, or providing the same address or telephone numbers as that provided by other customers that have previously conducted similar operations.

PROVISO: For the purpose of this article, the reference threshold for exchange bureaus will be one thousand balboas (B/.1,000.00).

ARTICLE 6. RED FLAGS RELATED TO PAPER MONEY CHARACTERISTICS. Reporting entities must pay special attention to the following behavior or actions related to paper money characteristics:

1. The request for high denomination bills or the exchange of cash in one currency for another, in operations whose amount seems not to be justified by what is known of the customer;

2. A customer trying to mix a real currency with counterfeit currency;

3. A customer exchanging currency and requesting banknotes of the highest denomination possible in a foreign currency;

4. The simultaneous exchange of different currencies, when there is no justification according to what is known of the customer;

5. A customer that begins to exchange high denomination bills for small denominations or vice-versa when he usually does not use cash as a means of payment;

6. A customer that tries to conduct the operation providing very dirty, wet, moldy or smelly bills (e.g. impregnated in chemical products).

ARTICLE 7. RED FLAGS RELATED TO THE ORIGIN OR DESTINATION OF THE OPERATION FOR WIRE TRANSFERS. Reporting entities must pay special attention to the following behavior or actions:

1. A customer sending wire transfers to a country different from his country of origin;

2. A customer receiving wire transfers form a country different from his country of origin;

3. Operations without an apparent business reason or not belonging to the customer's business or his operational background;

4. Operations coming from or going to countries or territories designated as high-risk countries for money laundering, the financing of terrorism and the financing of the proliferation of weapons of mass destruction and/or those not meeting FATF standards, or operations involving people residing in those countries;

5. Receiving one or more wire transfers for an amount under five thousand balboas (B/.5,000.00) ordered from any developed country, especially if containing any allusion to lotto or gambling prizes.

PROVISO: For the purpose of the above, the reference threshold for exchange bureaus will be one thousand balboas (B/.1,000.00).

ARTICLE 8. OTHER RED FLAGS. Reporting entities must pay special attention to the following behavior or actions:

1. Businessmen acting as customers receiving or sending wire transfers abroad for large amounts, as payments or collections for computer information, mobile phones or

similar, maintaining an significant operation over a short period of time and then terminating the relationships or replacing them with new companies;

2. Businessmen acting as customers making payments through wire transfers to a limited group of alleged suppliers with funds in the exact amount previously received in cash or through wire transfers from alleged customers;

3. A customer who is the beneficiary of small wire transfers ordered by individuals from abroad, but that together amount for a significant amount, without any appreciable business activity;

4. The refund or annulment of wire transfers issued or received;

5. Operations that seem to be connected to immigration and that are not frequently repeated;

6. Customers systematically making operations during business hours in which the establishments have a greater influx of customers, in order to avoid scrutiny;

7. Customers that, without apparent reason, receive huge amounts of money;

8. Wire transfers of payments or collections without apparent links to legitimate contracts, goods or services;

9. A customer conducting a wire transfer for an unusual amount compared to the amounts previously transferred;

10. Operations not matching the customer's financial activity or operations that do not appear to have a normal business objective;

11. A customer with an uncommon curiosity for the reporting entity's internal control measures and procedures related to money laundering, the financing of terrorism financing and the financing of the proliferation of weapons of mass destruction;

12. Customers acting evasively in regards to the operation;

13. The customer's unusual behavior, especially not being worried about wire transfer fees, or the applicable rate of exchange, even though the transfer involves large amounts of money or there are cheaper alternatives;

14. Virtual wire transfer management operations when there is a suspicion that the procedure is conducted to try to avoid the establishment's control or there are doubts as to the customer's identity;

15. A customer making usual operations in an establishment that is far from his job or residence;

16. A customer receiving many wire transfers for small amounts that orders a wire transfer or begins ordering wire transfers to another person in another city or country for an amount equal to the sum of the previous transfers on the same day or a few days later;

17. A customer that tries to bribe, force or induce an employee to fail to comply with any of the measures provided in the Law or by the entity itself related to the prevention of money laundering, the financing of terrorism and the financing of the proliferation of weapons of mass destruction;

18. A customer that refuses to provide the entity any additional information on himself that would permit him to access discounts, offers or programs for the establishment's preferential customers;

19. Currency exchange operations in a currency that does not belong to the customer's nationality of origin;

20. Customers making huge purchases of traveler's checks that are not related to travel plans;

21. A customer requesting that a lsrge amount of money in a foreign currency be exchanged for another foreign currency;

22. Frequent or significant exchanges of US dollars to foreign currencies or vice-versa without their being justified by the customer's professional or business activity;

23. Transactions for which the customer has no explanation;

24. The sudden growth in the amount and frequency of remittances sent by the customer;

25. Societies or charities that make occasional remittances of significant amounts of money to countries where there is no evidence that they are conducting regular activities and there is no information on a catastrophe or advertising campaign that would justify the collection and subsequent remittance of funds to these countries.

ARTICLE 9. RISKS RELATED TO SUSPICIOUS BEHAVIOR BY EMPLOYEES OR AGENTS OF THE REPORTING ENTITY. Reporting entities must pay special attention to the following behavior or actions:

1. An employee of a reporting entity having significant changes in his lifestyle, higher than that justified by his salary, or with sudden changes in his behavior, e.g. avoids taking vacations without a reasonable explanation;

2. An employee that has processed a large number of operations or transactions of an unusually high volume compared to others in the same establishment, which can indicate that he has agreed or been forced to provide services to one or more specific customers;

3. A reporting entity agent whose number of new customers is higher than usual compared to its existing customers, especially if the new customers' operations have characteristics different from those from the usual customers;

4. A reporting entity agent that has a larger volume of operations than the average volume of operations conducted by other agents of that reporting entity without having a reasonable explanation;

5. An agent conducting a volume of operations in a given destination for an average amount much greater than the average amount of operations conducted to that same destination by the remaining money service businesses agents;

6. An agent conducting a substantial volume of operations whose destination is the same city or geographical area, without justification;

7. An agent focusing his operations on short dates or unusual hours, without reasonable explanation;

8. An agent experiencing a significant increase in the volume of operations, without justification, especially if that increase is because of increases in operations coming from or going to a specific country;

9. An agent that classifies operations as immigrant remittances when it is observed that the surnames of the ordering parties frequently do not match those of the respective beneficiaries;

10. An agent having a substantial volume of operations in which the ordering parties and beneficiaries appear to be interrelated, without a reasonable cause, even though the different ordering parties are sending money to the same beneficiary or beneficiaries or different beneficiaries receive money from the same ordering party or parties;

11. An agent whose customers are ordering transfers to a greater number of beneficiaries than usual, or are receiving money from a greater number of ordering parties than usual;

12. An agent having a substantial volume of operations in which the ordering parties are identified with passports;

13. An agent with a high number of senders whose nationality or country of birth is different than the country of destination of the payment operations;

14. Agents with customer files that repeatedly include the same data or slightly altered data in certain fields (address, telephone, activity, etc.);

15. An agent with a high number of payment operations in which the beneficiaries declare receiving the money for the same reason, with that reason being unusual (e.g. purchasing a car);

16. Agents having operations allegedly conducted by the customers, when those customers have directly informed the reporting entity that they have not conducted those operations;

17. Agents for whom it is observed that the copies of the identification documents of the ordering parties were forged, altered or manipulated;

18. Agents not appropriately keeping the slips verifying the performance of an operation, or a substantial quantity of these slips not being signed by the senders, or the signatures do not match those on the identification documents of the senders;

19. Agents depositing funds from operations in the bank account of the money services businesses in advance;

20. Agents splitting deposits in the bank account of money service businesses to avoid identifying themselves, or at offices far from where they theoretically collect operations, or through income from third parties unknown to the money service businesses;

21. An agent acting as ordering party in money sending operations to different countries or beneficiaries;

22. Agents whose customers make a huge number of money remittance orders for amounts slightly under five thousand balboas (B/.5,000.00);

23. An agent who refuses to meet the reporting entity's internal control measures to prevent money laundering, the financing of terrorism and/or the financing of the proliferation of weapons of mass destruction, e.g. alleging that the measures established by other reporting entities are more permissive.

CHAPTER III
RED FLAGS RELATED TO THE FINANCING OF TERRORISM

ARTICLE 10. RED FLAGS RELATED TO THE FINANCING OF TERRORISM. Reporting entities must pay special attention to the following behavior or actions:

1. Customers with names, aliases, dates of birth and other specific indicators of persons involved in terrorism according to the specific national or international financial sanctions lists that may be related to existing customers, beneficiaries and commercial entities on file;

2. Customers providing addresses of people involved in terrorism, on specific national or international financial sanctions lists or that may be related to existing customers, beneficiaries and commercial entities on file;

3. Customers involved in terrorism, on specific national or international financial sanctions lists whose monies or other property may be related to other entities or customers;

4. Customers known or suspected of being involved in terrorist activities or as foreign terrorists;

5. The establishment of a permanent residence and/or frequently changing residence apparently unrelated to the declared operation;

6. Customers resisting the cultural standards of the country where they are conducting the operation and that make great efforts to avoid personal contact with some bank employees (e.g. refuses to interact with female employees);

7. Transactions coming from or going to jurisdictions or regions that are transit spots or that have had a flow of money from known foreign terrorists;

8. Excessive funds paid to an account held by a student in a foreign country by a family member or an unrelated organization;

9. A beneficiary constantly providing the address of a hotel in a tourist area as his personal address;

10. Real telephone numbers replaced by randomly generated phone numbers or logical sequences of numbers that could appear to be a national telephone number (e.g. 0123456789);

11. A high volume of operations conducted by a single person in different locations;

12. The sudden increase in the volume of operations by many persons during a short period of time in an establishment with a single agent,;

13. Operations coming from or going to cities identified as receiving an increasing number of wire transfers between periods of pre-crisis and active conflicts;

14. Customers conducting a huge volume of operations with many countries;

15. The same person receiving money from different money service businesses or locations of wire transfer service agents;

16. The customer seems to know the amount being transferred once the wire transfer employee counts the money;

17. The sent operation was not ever received by the beneficiary, who has supposedly passed away;

18. A customer changing a large amount of foreign money to domestic currency and, at the same time, transferring it to an area bordering an area of conflict;

19. Currency exchange operations followed in a short period of time by international wire transfers to high-risk jurisdictions.

ARTICLE 11. ENACTMENT. This Rule will become effective upon its promulgation.

Given in the city of Panama on the twenty-sixth (26th) day of March, two thousand and nineteen (2019).

FOR COMMUNICATION PUBLICATION AND ENFORCEMENT.

THE CHAIRMAN, **THE SECRETARY,**

Luis Alberto La Rocca Joseph Fidanque III